3. Information Protection

This chapter includes system and information security standards and guidance. The relationship of this chapter with the ITSG is shown in Figure 3-1.

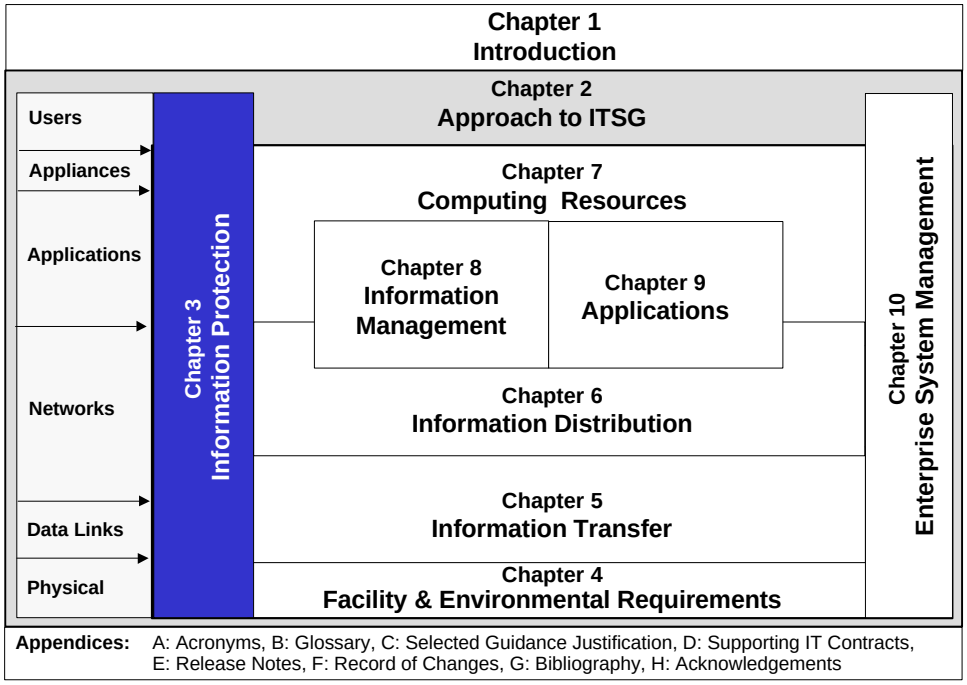

Figure 3-1. ITSG Document Map Highlighting Chapter 3, Information Protection

3.1 Overview

This chapter provides the information protection standards guidance necessary to implement secure information systems while ensuring interoperability. The standards, identified in the "best practices" paragraphs, apply to all DON automated information systems.

3.2 Background

DON information systems must have adequate safeguards, both technical and procedural, to ensure the security of data processed. System safeguards must provide information protections commensurate with the security requirements of the data processed in a particular information system. In general, DON information systems should provide appropriate safeguards to ensure the confidentiality, integrity, availability, authenticity, and non-repudiation of information processed. The actual safeguards used should be commensurate with the operational requirements, information sensitivity level, and consequences of exploitation of the specific DON information system.

Most modern DON information systems are rapidly developed and fielded in an evolutionary manner. The majority of these systems are intended to be connected to LANs and use WANs (e.g. the NIPRNET or SIPRNET) as a primary data transport mechanism. Unfortunately, these LAN/WAN connections can be exploited by an adversary attempting to compromise DON information and information systems. Providing an adequate level of information protection at an

acceptable cost is difficult in this type of environment. Recent experience in the DON, DOD, and private industry has shown that the best solution to this problem is to use a defense in depth approach to information protection.

Defense in depth is provided by employing multiple security mechanisms at various locations (both physical and logical) in an information system. These mechanisms are applied in both a complementary and redundant manner to satisfy the information system's security requirements. No single mechanism is relied upon to provide complete information security. To compromise the security of a DON information system, an adversary must defeat the security mechanisms, "layer-by-layer." Defense in depth is extremely beneficial because most modern DON information systems are composed of COTS operating systems (OS) and applications, and these are regularly discovered to have subtle security flaws. With proper defense in depth, the risk is minimized that a single security flaw in an OS or application will leave an information system vulnerable.

3.3 Information Protection Requirements

Information protection requirements must be defined for each DON information system. The specific requirements are derived from the operational concept of an information system and take into account the system mission, sensitivity of the information processed, and the possible consequences of compromise. The information protection requirements are documented in the information system's security policy. At a minimum, the information system security policy specifies the system-specific information protection requirements in the following areas:

Confidentiality – The protection of classified and sensitive unclassified information from unauthorized disclosure.

Integrity – The protection of information and information system resources from unauthorized, undetected modification.

Availability – The assurance that authorized users will have reliable and timely access to required resources (including information, system services, communication services, etc.).

Authenticity – The ability to determine if information was created or modified by an authorized entity.

Non-repudiation – The ability to provide non-forgeable proof of a data originator's identity and non-forgeable proof of data receipt.

Employing information protection measures satisfies these information protection requirements. There are six broad categories of information protection mechanisms.

Encryption – Converting understandable information into unintelligible data for storage and transport in potentially hostile environments and then restoring this information (decryption) to authorized users.

Access Control – Controlling access to system data and resources based on a user's identity or operational role.

User Identification and Authentication (I&A) – Securely determining a user's identity or operational role.

Malicious Content Detection – Examining incoming data to detect and block malicious content (e.g., viruses).

Audit – Recording security-relevant events in a protected form (for use in non-real-time event reconstruction as well as in real-time intrusion detection).

Physical and Environmental Controls – Policies, procedures, and mechanisms related to physically protecting and providing for continuity of operations for system components. These are addressed in Chapter 4.

To achieve information protection over the DON enterprise, the information architecture can be categorized in dimensions that must be protected. The top level dimensions listed from the more general to the specific are:

Information System – The actual infrastructure itself must be protected against unauthorized intrusion and denial of service.

Information Domain – Communities-of-interest within the infrastructure must be afforded freedom to move and process information within a virtual enclave that provides protection.

Information Content – Information packages themselves have to be protected against unauthorized access by untrusted users both in-transit and at rest (in storage).

Figure 3-2 is a summary of the dimensions and components used to provide information protection. Each dimension is shown as a matrix of information protection requirements (confidentiality, et al) versus information protection measures (encryption, et al). Within each cell of the matrix are components that are used to effect the information protection measures. The concept of these dimensions allows flexible release of some information elements to selected trusted users while protecting the rest of the information from those who do not have a need to know. A defense-in-depth strategy is used to layer security measures at each perimeter of the infrastructure. A collection of security components is used to establish the protection needed at each zone for each information protection dimension.

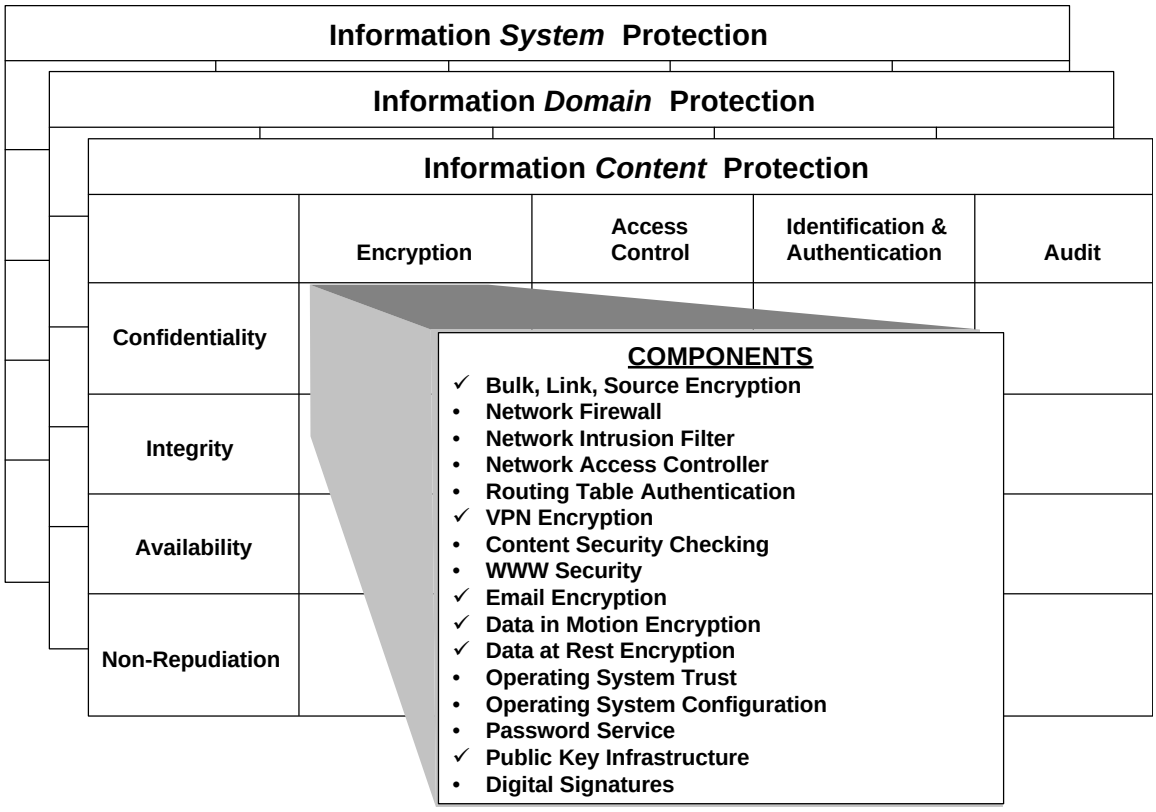

Figure 3-2. Information Protection Summary

3.4 Defense in Depth Approach

In defense in depth, security protection mechanisms are employed in a layered fashion, at multiple locations in a system architecture. This ensures that DON systems maximize resistance to attacks and minimize the probability of a security breach due to a weakness (known or unknown) in any single security mechanism.

The defense in depth information protection concept is directly analogous to sea control concepts. Fleet air defense can serve as a representative example. The outer zone is defended by intercept fighters such as F-14s and controlled by E-2Cs; a second layer of defense is the missile zone defended by Aegis cruisers; they intercept attackers that have not been defeated by the outer layer. Inside the missile zone lie the point defense zones where the defensive weapons include chaff, close in warfare systems and tactical electronic warfare machinery. If the system is working properly, the number of leakers that penetrate to the inner zone is less than the capacity of the point defense weapons.

A generic framework for defense in depth is illustrated in Figure 3-3. Four zones of defense are defined in this framework. It is important to note that the zones of defense may be logical and not necessarily physically separate. It should also be noted that the selection, placement, and configuration of particular security mechanisms are implementation dependent. The type and strength of security mechanisms are driven by the information protection requirements for a particular DON information system.

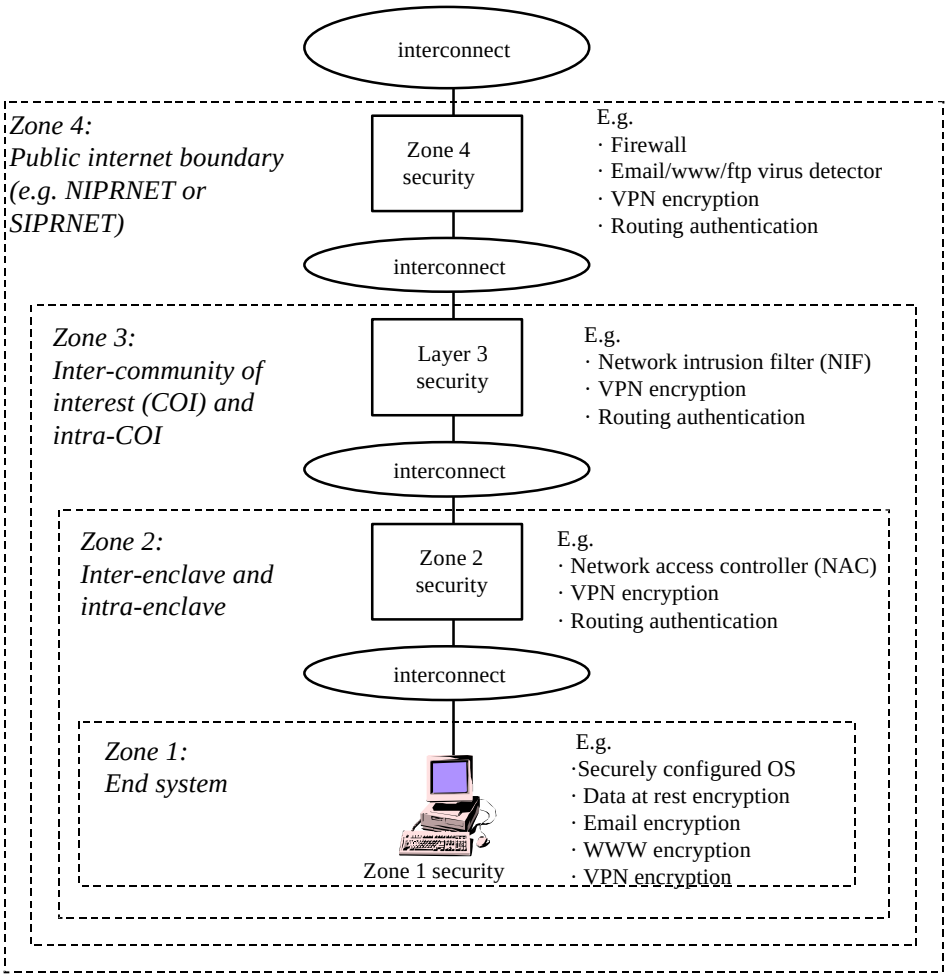

Figure 3-3. Defense in Depth Concept

In addition to the information protection mechanisms, certain infrastructure components are required to build secure DON information systems. The most critical of these components is a public key infrastructure (PKI) that can be applied in the various zones to support identification and authentication mechanisms and encryption mechanisms.

Figure 3-4 summarizes how information protection components are applied to each architecture security zone and information dimension. The role of each in protecting the information and infrastructure is provided below.

	Info System	Info Domain	Info Content	ZONE 1	ZONE 2	ZONE 3	ZONE 4
Bulk, Link, Source Encryption	C,I,a	C,I,a	C,I,a				✓
VPN Encryption	C,I,a	C,I,a	C,I,a	✓	✓	✓	✓
Data at Rest Encryption		C,I,a	C,I,a	✓			
WWW Encryption		C,I,a	C,I,a	✓			
Email Encryption			C,I,a,N	✓			
Digital Signatures			C,I,a,N	✓			
Routing Table Authentication	A,a	A,a			✓	✓	✓
Public Key Infrastructure		☑	☑	☑			
Network Firewall	C,I,A,a	C,I,A,a			◯	◯	✓
Network Intrusion Filter	C,I,A,a	C,I,A,a			◯	✓	◯
Network Access Controller	C,I,A,a	C,I,A,a			✓		
Content Security Checking		I,A	I,A	✓	◯	◯	✓
Operating System Security	C,I,A,a	C,I,A,a	C,I,A,a	✓			
Operating System Configuration	C,I,A,a	C,I,A,a	C,I,A,a	✓			
Password Service	a	a	a	✓			✓

C confidentiality **a** authenticity
I integrity **N** non-repudiation
A availability

✓ **applicable** ◯ **optional**
☑ **infrastructure component**

Figure 3-4. Security Components Applied to Architecture Dimensions and Protection Zones

3.4.1 Zone 4 Protection Mechanisms

Zone 4 information protection mechanisms are employed at the boundary between a DON information system (or multiple DON information systems connected by a private intranet) and a public internetwork (e.g. NIPRNET, SIPRNET). Zone 4 information protection mechanisms may include:

- Network firewalls
- Virtual Private Network (VPN) encryption
- Content security checking
- Routing table update authentication

3.4.1.1 Network Firewall

The most effective zone 4 information protection mechanism is the properly configured and managed network firewall. A firewall is a collection of hardware and software components that is used to selectively allow external entities (e.g. users on the Internet) access to information systems located “behind” the firewall. A firewall is installed between an information system (or intranetted systems) and a public internetwork. In addition to providing network access control, a properly configured and managed firewall can provide network intrusion prevention.

There are three primary categories of network firewalls:

- Packet filter

- Stateful packet filter
- Application layer gateway

A packet filter firewall uses a conventional filtering IP router to implement Access Control Lists (ACLs) to restrict incoming and outgoing connections based on the service type and the source/destination of the connections. A packet filter is considered to be the least capable and least secure type of network firewall. A stateful packet filter firewall is similar to a packet filter but it can also use knowledge of higher level protocols to identify and allow legitimate protocols, and to identify and disallow certain network attacks. A stateful packet filter firewall is considered more secure than a packet filter firewall. An application layer gateway firewall, also known as a bastion host firewall, examines incoming and outgoing connections at the application layer using proxies. These proxies can force incoming connections to be authenticated at the firewall as well as blocking most known network attacks. An application layer gateway firewall is considered the most secure network firewall.

Because of the associated expense and management overhead, network firewalls may be installed in central locations (e.g., a regional information technology service center) and shared by DON information systems connected via a private intranet.

Best Practices

All DON information systems should use application layer gateway network firewalls to secure connections to public internetworks. Network firewalls can be centrally located, centrally managed, and shared between multiple sites only if a secure intranet is used to connect the sites. A Memorandum of Agreement (MOA) may be required between the DON activities that share a network firewall. The MOA should state the firewall policies that specify the network services to be allowed (see Figure 3-5 for representative services).

Application layer gateway network firewalls procured for DON information systems should, at a minimum, provide support for the following network applications: SMTP, HTTP, HTTPS, SSL, gopher, NNTP, telnet, FTP, and RealAudio. Network firewalls at a minimum should support secure, non-spoofable, user authentication across a network-MD5 based Skey. Network firewalls should support integration with one of the products on the DoD virus tool site license (see Section 3.4.1.3) using the Open Platform for Secure Enterprise Connectivity (OPSEC) Content Vectoring Protocol (CVP). If a virtual private network (VPN) encryption capability is required, it should conform to policies specified in Section 3.4.1.2 of this document.

Network firewalls should be configured with the most restrictive security policy possible, “that which is not expressly allowed is denied.” Figure 3-5 identifies a baseline of network services that either can, can conditionally (based on system specific requirements), or cannot securely be allowed through a network firewall. It should be noted that although specific protocols may not have a first order negative impact on system security, their use by DON systems may lead to inadvertent denial of service due to resource consumption. As a result, DAAs need to consider if the operational requirement for a particular protocol justifies the potential negative impact on network resources. Detailed guidance documenting the vulnerabilities and risks associated with allowing specific network services to traverse a network firewall can be found in “Firewall Services,” SPAWAR PMW-161 report, December 1996. This report can be accessed at: ftp://infosec.navy.mil/pub/docs/navy/NSS/firewalls/fw_serv.doc.

DON information systems must ensure that any protocols used across public internetworks are compatible with application layer gateway network firewalls. Guidance for determining this compatibility is identified in the “Firewall Services” document.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	Application layer gateway network firewall	Application layer gateway network firewall	Application layer gateway network firewall	Application layer gateway network firewall	
Activities, Platforms, Operational Environments		ITSCs and Shore Information Producer Commands, Shore Commands connected directly to a WAN			

Table 3-1. Zone 4 Firewall Recommended Implementations

Service	Allow in	Comments	Allow out	Comments
DNS	Yes	Split server	Yes	Split server
SMTP	Yes	Secured mail forwarder	Yes	Secured Mail Forwarder
TELNET	Yes	Proxy with strong authentication	Yes	Proxy
HTTP	Yes	Proxy with strong auth., external server, split server Block ActiveX Conditionally allow Java	Yes	Proxy, IP address filter, Split Server
HTTPS (SSL)	Yes	Proxy, external server, split server Block ActiveX Conditionally allow Java	Yes	Proxy, IP address filter, Split Server
RealAudio™	Yes	Proxy	Yes	Proxy
Lotus Notes	Yes	Generic proxy, IP port filter	Yes	Generic Proxy, IP Port Filter
FTP	Yes	Proxy, strong authentication	Yes	Proxy
WAIS	Cond.	Split server	Yes	Proxy
Anonymous FTP	Cond.	Server external to firewall	Yes	Proxy
SQL*Net	Cond.	Proxy with strong authentication	Yes	Stateful packet filter, proxy
Gopher	Cond	External server, split server	Yes	Proxy, IP address filter, Split Server
NNTP	Cond.	External server, generic proxy	Yes	Generic Proxy
ICMP	Cond.	Block “echo request,” “time to live exceeded,” “redirect.”	Cond.	Block “echo reply,” “time to live exceeded,” “redirect.”
X.400	Cond.	Generic proxy	Cond.	Generic Proxy
X.500	Cond.	Generic proxy, IP port filter	Cond.	Generic Proxy IP Port Filter
DMS	Cond.	Split server	Cond.	Split server
POP3 and IMAP4	Cond.	Proxy with strong authentication	Cond.	Proxy
‘r’ commands	Cond.	Proxy with strong authentication	Cond.	Proxy

Service	Allow in	Comments	Allow out	Comments
IRC	Cond.	Generic Proxy, IP Port Filter	Cond.	Generic Proxy, IP Port Filter
T.120/H.323	Cond.	Generic Proxy, IP Port Filter	Cond.	Generic Proxy, IP Port Filter
Syslog	Cond.	Log at firewall, limit to external router and DON servers inside external router using packet filters	No	
SNMP	No		Cond.	Two mgmt. stations, IP Address Filter, proxy
Finger	No		Cond.	safe_finger
X-Windows	No		Cond.	IP Address Filter
Printing	No		Cond.	Proxy
NTP	No		No	
Microsoft RPC	No		No	
NETBIOS	No		No	
NIS	No		No	
RPC	No		No	
Archie	No		No	
TFTP	No		No	
NFS	No		No	
Talk	No		No	
MBONE	No		No	

Cond. = conditional; service may be acceptable based on system specific requirements

Figure 3-5. Allowable Services for Network Firewalls

3.4.1.2 Virtual Private Network (VPN) Encryption

VPN encryption can be used to provide confidentiality and integrity of data transmitted across a public internetwork. In addition, VPN encryption can provide authentication of the remote system that encrypted the data. When integrated into suitable system architectures, VPN encryption allows secure “tunnels” to be established across insecure internetworks. This allows a private intranet to run (securely) over a public internet.

The National Security Agency (NSA) evaluates the strength of cryptographic devices intended to secure classified data. A VPN encryption device endorsed by NSA for Type 1 applications can be used to encrypt classified networks, providing a resulting data stream that can be treated as unclassified. The NSA endorsed Type 1 devices allow VPN encryption at the IP or ATM layers.

- For IP encryption, there are currently only two NSA endorsed devices – the Network Encryption System (NES) and the Embeddable INFOSEC Product (EIP). NES is a COTS device produced by Motorola. Unfortunately, the NES has performance and key management limitations that have made deployment difficult. EIP is a GOTS device that is centrally procured by OPNAV N6. EIP has not yet been operationally employed and is currently only available in limited quantities.
- For ATM encryption, the only device currently endorsed by NSA, is the Fastlane (KG-75). In FY99, NSA expects to release (and shortly thereafter endorse) a device that will be capable of providing both IP and ATM layer encryption. This device, the Taclane, is expected to overcome the limitations associated with the NES in the IP encryption mode. It will not be interoperable with the NES or EIP in IP layer encryption mode. It will be interoperable with the Fastlane in ATM layer encryption mode, but will operate only at DS-3 rates.

Many commercial vendors produce software and hardware that can provide VPN encryption for unclassified or sensitive but unclassified data. Recently, a number of vendors have developed VPN encryption based on the IP security (IPSEC) standard. IPSEC can provide data confidentiality, integrity, and authentication by encrypting packets at the IP layer.

The IPSEC standard has been designed to allow for "drop-in" employment of encryption algorithms.[1] For data confidentiality, IPSEC currently supports various algorithms including DES, 3DES, RC5, IDEA, CAST128, and Blowfish. For data integrity and authentication, IPSEC currently supports keyed MD5 and SHA-1. The IPSEC standard also allows for employment of various key management and distribution schemes. The simplest is based on manual pre-placement of key material. The Internet Security Association and Key Management Protocol (ISAKMP)/Oakley provides more automated and scalable key management and distribution.

Best Practices

Classified data that is encrypted with VPN techniques must be handled at its original classification level unless an NSA-endorsed Type 1 (designed to secure classified information) cryptographic device is used. If declassification of data is required (e.g. to allow for transmission over non-secure networks), an NSA-endorsed device must be used. Requirements for NSA-endorsed cryptographic devices must be submitted to CNO N643 for validation. Many NSA-endorsed cryptographic devices are centrally procured by SPAWAR PMW-161.

COTS VPN mechanisms may be used for encryption of unclassified data, and of classified data that will be handled at its original level (e.g., for privacy of secret data across the SIPRNET). To provide for interoperability, IPSEC based mechanisms will be used if available. IPSEC mechanisms will utilize DES or 3DES for encryption. FIPS 140-1 certification of DES implementations is recommended. Keyed SHA-1 for data authentication and integrity is preferred, but keyed MD5 is an acceptable substitute if SHA-1 is not available. Additional information on the use of commercial cryptography in DON systems is provided in Section 3.6. An acceptable option for key management and distribution is a preplaced secret key.

[1] An overview of cryptography and DON standards/guidance for cryptography is presented in section 3.6. Standards and guidance provided in section 3.6 apply to all infrastructure components and information protection mechanisms that make use of cryptography.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
Proprietary VPN products	IPSEC with • DES or 3DES • SHA-1 or MD5 • Preplaced key or ISAKMP/ Oakley	IPSEC with • DES or 3DES • SHA-1 • Preplaced key or ISAKMP/ Oakley	IPSEC with • DES or 3DES • SHA-1 • Preplaced key or ISAKMP/ Oakley	IPSEC with • DES or 3DES • SHA-1 • Preplaced key or ISAKMP/ Oakley	
Activities, Platforms, Operational Environments		ITSCs and Shore Information Producer Commands, Shore Commands connected directly to a WAN			

Table 3-2. Zone 4 VPN Implementations

3.4.1.3 Content Security Checking

Many forms of computer information can contain harmful content including viruses, macro viruses, Trojan horse programs, etc. These “malicious programs” can be transmitted across a network in a number of ways including SMTP e-mail attachments, FTP file downloads, and Java applets. Incoming data can be checked for harmful content at the public internetwork boundary.

Numerous COTS products exist that can perform this type of content security checking. These products can be integrated with a zone 4 network firewall system. Two such products, Norton and McAfee, are available on the DoD-wide virus detection tool site license (see http://infosec.navy.mil/)

Best Practices

All DON information systems should employ content security checking mechanisms for e-mail with attachments, FTP data, and http data incoming from a public internetwork. Products from the DoD wide virus detection tool site license should be used. Updated virus detection signatures should be downloaded and installed monthly from the http://infosec.navy.mil or http://infosec.navy.smil.mil web site.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	DoD site license virus detection tools	DoD site license virus detection tools	DoD site license virus detection tools	DoD site license virus detection tools	
Activities, Platforms, Operational Environments		ITSCs and Shore Information Producer Commands, Shore Commands connected directly to a WAN			

Table 3-3. Zone 4 Content Security Checking Implementations

3.4.1.4 Routing Table Update Authentication

IP routers are used to connect LANs and/or MANs to public internetworks. Routers connected to public internetworks must regularly exchange routing table updates across these internetworks. These routing table updates can be spoofed in transmission or forged, thus resulting in denial of service or possibly a network intrusion. Many COTS IP routers feature cryptographic authentication of updates for selected routing protocols. These features can often be used by simply reconfiguring existing routers.

Currently, the BGP and OSPF routing protocols support cryptographic authentication. These routing protocols use a keyed MD5 hash algorithm to provide the cryptographic authentication. Due to weakness in the MD5 algorithm, SHA-1 will likely begin to appear as an option for cryptographic authentication of routing protocols.

Best Practices

All IP routers procured for DON information systems should feature, at a minimum, keyed MD5 authentication for BGP, and OSPF routing protocols. Keyed MD5 authentication should be used between all DON IP routers where possible.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
Unauthenticated routing protocols	BGP and OSPF with MD5 authentication	BGP and OSPF with MD5 authentication	BGP and OSPF with MD5 authentication	BGP and OSPF with MD5 authentication	BGP and OSPF with SHA-1 authentication
Activities, Platforms, Operational Environments		ITSCs and Shore Information Producer Commands, Shore Commands connected directly to a WAN			

Table 3-4. Zone 4 Routing Table Security Implementations

3.4.2 Zone 3 Information Protection Mechanisms

Zone 3 information protection mechanisms are used to provide inter-community of interest (COI) and intra-COI security. In general, zone 3 information protection mechanisms are installed as part of an intranet used to connect end user networks that have similar security requirements and have a common COI. Zone 3 information protection mechanisms may include:

- Network Intrusion Filters (NIF)
- Network firewalls
- VPN encryption
- Content security checking

3.4.2.1 Network Intrusion Filter (NIF)

For high value COIs, a strong layer of defense can be provided by a network intrusion filter. A NIF may be less restrictive than a zone 4 firewall and thereby allow a wider range of network applications to be used, both internal to and across the COI boundary. However, a NIF can detect a wide variety of network attacks and block these attacks. Certain classes of NIFs, known as intrusion detection systems, can provide real time reporting to local security managers and/or to the Fleet Information Warfare Center (FIWC).

Several vendors are currently producing products suitable for NIF applications. These products include stateful filtering routers and active intrusion detection systems.

Stateful filtering routers are similar to normal filtering IP routers. They can be used to allow or disallow incoming packets based on source/destination IP addresses and source/destination TCP ports. In addition, stateful filtering routers use knowledge of higher level protocols to identify and allow legitimate protocols, and to identify and disallow certain network attacks.

Active Intrusion Detection Systems (IDS) also use knowledge of higher level protocols to identify network attacks. When an attack is detected, it can be reported to a central monitoring facility and possibly blocked (e.g., using a TCP connection reset). Depending on its configuration, an active IDS may be able to provide a high level of security in a non-intrusive manner.

Best Practices

Use Network Intrusion Filters to provide information protection mechanisms. No standards currently exist.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	Stateful filtering router Active intrusion detection system	Stateful filtering router Active intrusion detection system	Stateful filtering router Active intrusion detection system	Stateful filtering router Active intrusion detection system	
Activities, Platforms, Operational Environments		ITSCs and Shore Information Producer Commands, COIs with strong security requirements			

Table 3-5. Zone 3 Network Intrusion Detector Implementations

3.4.2.2 Network Firewall

COIs with extremely high security requirements may employ network firewalls at zone 3. This will provide increased security but may limit the range of network applications that can be used intra-COI and (more likely) inter-COI. See Section 3.4.1.1 for guidance on network firewalls.

3.4.2.3 VPN Encryption

VPN encryption may be employed at zone 3 to provide COI security across a DON intranet shared with other COIs and/or across a public internetwork. See Section 3.4.1.2 for guidance on VPN encryption.

3.4.2.4 Content Security Checking

Content security checking may be employed at zone 3 to protect entire COIs. See Section 3.4.1.3 for guidance on content security checking.

3.4.3 Zone 2 Information Protection Mechanisms

Zone 2 information protection mechanisms are used to provide security at the boundary to a single site or enclave and on the LAN for the site or enclave. Zone 2 mechanisms are generally integrated as part of the site/enclave LAN. Zone 2 information protection mechanisms may include:

- Network Access Controllers (NAC)
- NIFs
- Network firewalls
- VPN encryption
- Content security checking

3.4.3.1 Network Access Controller (NAC)

A network access controller provides a basic level of access control over network connections based on a site/enclave's local security policy. These controls could include restrictions on incoming connections as well as on connections between LAN segments internal to the site/enclave. These restrictions could be based on the source and destination addresses of the IP packet as well as the service type (e.g., SMTP e-mail, telnet, HTTP). A NAC could be implemented using the organic filtering IP routers used to connect the site/enclave to the external world. For ATM systems featuring "cut through" routing, filtering ATM switches (being developed by at least one vendor) could be used to implement a NAC.

Best Practices

IP routers procured for DON information systems should have the capability to perform IP packet filtering. At a minimum, routers should be able to accept/reject packets based on protocol type, source IP address, destination IP address, source TCP/UDP port, destination TCP/UDP port, and TCP established bit. Routers should be able to audit IP packets rejected by packet filters.

Currently, few options exist for filtering ATM switches. However, as products become available, selection criteria should be similar to that for filtering IP routers (see previous paragraph).

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	Filtering IP router	Filtering IP router	Filtering IP router	Filtering IP router	Filtering ATM switch
Activities, Platforms, Operational Environments		All			

Table 3-6. Zone 2 Network Access Controller Implementations

3.4.3.2 Network Firewall and NIF

Sites/enclaves with extremely high security requirements may employ NIFs or network firewalls at zone 2. This will provide increased security but will increase cost and management overhead. In addition, a network firewall may limit the range of network applications that can be used across the site/enclave boundary. See Section 3.4.1.1 for guidance on network firewalls and Section 3.4.2.1 for guidance on NIFs.

3.4.3.3 VPN Encryption

VPN encryption may be employed at zone 2 to provide COI security across a DON intranet shared with other COIs and/or across a public internetwork. See Section 3.4.1.2 for guidance on VPN encryption.

3.4.3.4 Content Security Checking

Content security checking may be employed at zone 3 to protect entire sites/enclaves. See Section 3.4.1.3 for guidance on content security checking.

3.4.4 Zone 1 Information Protection Mechanisms

Zone 1 information protection mechanisms provide the inner-most layer of defense for DON information systems. The protections are implemented on the actual end systems including NT workstations, NT servers, UNIX servers, and mainframes. Zone 1 information protection mechanisms may include:

- Secure operating systems with secure configurations
- Data at rest encryption
- E-mail encryption
- World Wide Web (WWW) encryption
- VPN encryption
- Content security checking

3.4.4.1 Operating System Security Features and Configuration

Computer operating systems used in DON information systems should include features that allow the operating systems to provide access control for all information stored or processed. The National Security Agency (NSA) provides specification for security features and criteria for their

evaluation in DoD 5200.28-STD, commonly known as the Orange Book. The Orange Book C2 level specifies the minimum features required to provide access control in a multi-user environment: user identification and authentication, discretionary access control (DAC) with object reuse, and audit. An interpretation of the Orange Book C2 level requirements for DON information systems is provided in DON NAVSO P-5239-15 “Controlled Access Protection (CAP) Guidebook.”

Many COTS operating systems have been designed to meet C2 level requirements and some have been formally evaluated by NSA. Microsoft Windows NT 3.5 has been formally evaluated to meet C2 level requirements by NSA. Microsoft is currently seeking a formal NSA evaluation of NT 4.0 and has indicated formal evaluation will be sought for NT 5.0. Netware 4.11 has been formally evaluated to meet C2 level requirements by NSA and it is anticipated that Netware 5.0 will be entered into formal evaluation as well. Older versions of UNIX operating systems from various vendors have been formally evaluated to the C2 level by NSA. The current versions of most vendors’ UNIX operating systems have not been formally evaluated by NSA. However, these versions of UNIX generally contain C2 level features.

Security features of operating systems should be configured in a standardized manner to provide the highest level of security possible. These configurations should be periodically checked via an automated mechanism and reapplied as required.

Operating systems that do not contain C2 level security features (including Windows 3.1, DOS, Windows 95, Windows 98, Macintosh OS) should be avoided if possible. However, in situations where a PC will be normally used by a single person with no or limited network connections (e.g. a laptop), these operating systems may be acceptable if operating systems with C2 level features cannot meet the system functional requirements. Consult DON NAVSO P-5239-15 for detailed information that can be used in making such a determination.

DON information systems using Windows NT 4.0 (workstation and server) should be configured according to Naval standard configuration guidance. This guidance is documented in “Secure Windows NT Installation and Configuration Guide,” SPAWAR PMW-161 report, November 1997 (or the latest version). This report can be accessed at ftp://infosec.navy.mil/pub/docs/navy/NT-SECURITY/navynt.zip

DON information systems using UNIX should follow best commercial practices for security configuration. Information on this topic can be accessed at: ftp://infosec.navy.mil/pub/docs/unix/.

Best Practices

Computer operating systems used in DON information systems should include C2 level security features. Formal NSA C2 evaluation is not required but is desirable. DON NAVSO P-5239-15 should be used in determining the suitability of a particular operating system.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
Operating Systems without C2 features	Windows NT 3.5/4.0 Netware 4.11 UNIX	Windows NT 4.0 Netware 4.11/5.0 UNIX	Windows NT 4.0/5.0 Netware 4.11/5.0 UNIX	Windows NT 4.0/5.0 Netware 4.11/5.0 UNIX	
Activities, Platforms, Operational Environments	All				

Table 3-7. Operating System Security Implementations

3.4.4.2 Application Layer Data at Rest Encryption

Encryption of data files stored on a workstation or server can provide defense against unauthorized access attempts originating both locally (e.g. browsing) and remotely (e.g. hacking across the Internet). Numerous COTS software and software/hardware-based encryption products are available. Most products can be configured to encrypt either on command or automatically (on file open and close).

Although many COTS data at rest encryption products utilize standard algorithms for encryption (e.g. DES), no standards exist for encrypted file formats. This makes interoperability between products impossible.

Best Practices

DON information systems that make use of data at rest encryption products should only employ products that use the following symmetric data encryption algorithms: DES, Triple DES (3DES), or Skipjack. See Section 3.6.2 for more information on acceptable encryption algorithms.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
Products with proprietary encryption algorithms	DES, 3DES, or Skipjack based products	DES, 3DES, or Skipjack based products	DES, 3DES, or Skipjack based products	DES, 3DES, or Skipjack based products	
Activities, Platforms, Operational Environments	All				

Table 3-8. Data at Rest Encryption Implementations

3.4.4.3 E-mail Encryption

Encryption can be employed by various applications to provide confidentiality, integrity, authentication, and non-repudiation for information transmitted across a network. One of the best

examples of this is application layer encryption of internet e-mail with attachments. Numerous COTS products exist that provide e-mail encryption. Some are based on proprietary schemes for encryption and limit interoperability. However, standards for e-mail encryption are now appearing along with interoperable products based on these standards.

Secure MIME (S/MIME) provides a developing set of standards for security of internet e-mail with attachments. S/MIME provides for the authentication of the mail sender and the protection of the integrity of the message content (both provided via a digital signature). It also provides for the confidentiality of the message body (provided by encrypting the message). The digital signature and the key are both based on public key cryptography. The encryption of the message body is based on symmetric cryptography.

S/MIME Version 2 is widely implemented and a number of vendors have passed interoperability tests. S/MIME v2 has not been approved by any recognized standards body; the standard is published as two documents called Internet-drafts by a group of e-mail and security software vendors. For a variety of reasons, S/MIME v2 will not become an Internet (IETF) standard, but as a de facto standard is supported by many popular e-mail products.

The next version of S/MIME (version 3) is being developed by the IETF S/MIME working group and is expected to become an IETF standard. This version of S/MIME may be used in web browsers and other Internet applications (for instance to allow the signing of documents) as well as in electronic mail. S/MIME version 3 is not yet available in commercial products. However, the standardization process is proceeding rapidly and may be in products in 1999. This ITSG classifies S/MIME v3 as an emerging standard.

Best Practices

E-mail encryption deployed in DON information systems should avoid proprietary solutions that preclude interoperability. Deploy only S/MIME-based solutions (currently S/MIME v2, possibly S/MIME v3 in the future).

In order to ensure that Naval organizations can trust the digital signatures in S/MIME messages, the digital certificates used must come from a Certificate Authority (CA) recognized by the Navy and Marine Corps as conforming to acceptable certificate issuance practices. Navy and Marine Corps organizations interested in CA pilot projects should contact the Navy INFOSEC Program Office, SPAWAR PMW-161. The S/MIME clients should be configured to recognize only the conforming certificate authorities. Many S/MIME clients come configured to recognize many of the current commercial certificate authorities; these may or may not conform to DoD or Naval CA standards.

Users of S/MIME v2 should be trained to check the identity of the signer (usually by examining the certificate that arrived with the e-mail), and to check the proper Certificate Revocation List (CRL) on the proper directory to ensure that the certificate used has not been revoked.

The cryptographic options selected should be from the following list since not all of the cryptography available in S/MIME v2 products is sufficiently strong to be used for DON applications. The following options are acceptable:

- DES EDE3 encryption in Cipher Block Chaining (CBC) mode with a 168-bit key (Triple DES or 3DES)
- DES encryption in CBC mode with a 56-bit key

The following S/MIME v2 encryption options should be considered UNACCEPTABLE for DON use:

- RC2 encryption in CBC mode with a 128-bit key
- RC2 encryption in CBC mode with a 64-bit key
- RC2 encryption in CBC mode with a 40-bit key

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
Proprietary e-mail encryption products SMIME with RC2 encryption	SMIME with DES or 3DES encryption	SMIME with DES or 3DES encryption	SMIME with DES or 3DES encryption	SMIME with DES or 3DES encryption	SMIME v3
Activities, Platforms, Operational Environments		All			

Table 3-9. E-mail Encryption Implementations

3.4.4.4 World Wide Web (WWW) Encryption

Another application that can significantly benefit from application layer encryption is WWW. Extensive deployment of WWW servers for both tactical and non-tactical applications is ongoing. The *Secure Sockets Layer (SSL)* protocol provides for both parties in a web-based transaction to authenticate each other and to hide communication via encryption of the information flowing between server and client. SSL can provide for fine-grained access control to web sites (by requiring a user to provide a valid certificate) and signatures, authenticity and privacy for transactions involving web browsers and servers. An interesting feature of SSL is that for the transaction in which the browser user's identity is not important, but encryption of the transaction and the authenticity of the web server are, only the server needs a valid certificate.

SSL v2 was the first widely deployed version of SSL. Most web servers and web browsers support SSL v2. It has been replaced by SSL v3, but not all servers and/or browsers support v3, although all current version browsers and servers support v3. It is a de facto standard, rather than one issued by a recognized standards body, but it is widely deployed.

Best Practices

Navy and Marine Corps web browsers and servers that use SSL should be configured to enable SSL v3 only. However, in those limited situations in which SSL v2 must be used, only the modes that employ stronger encryption should be used. Commands should move as rapidly as possible to products that use SSL v3; SSL v2 will only be acceptable for use for a limited time. Considerations for certificate issuance are similar to those for S/MIME systems (see Section 3.4.4.3).

Versions of web browsers or servers sold for export are not acceptable for use in the Navy and Marine Corps because of their lack of strong encryption. Web browsers or servers that

incorporate stronger encryption generally also include weak encryption. The browser should be configured so that weak encryption is not allowed.

In the web browser or web server, the following options for SSL v2 are acceptable:

- Triple DES (3DES) encryption with a 168-bit key
- DES encryption with a 56-bit key

The following options should be considered UNACCEPTABLE for DON use of SSL v2:

- RC4 encryption with a 128-bit key
- RC2 encryption with a 128-bit key
- RC4 encryption with a 40-bit key
- RC2 encryption with a 40-bit key

In the web browser or server, the following options for SSL v3 are acceptable:

- Triple DES (3DES) encryption with a 168-bit key and a SHA-1 MAC
- DES encryption with a 56-bit key and a SHA-1 MAC

The following options should be considered UNACCEPTABLE for DON use of SSL v3:

- RC4 encryption with a 128-bit key and an MD5 MAC
- RC4 encryption with a 40-bit key and an MD5 MAC
- RC2 encryption with a 40-bit key and an MD5 MAC
- No encryption with an MD5 MAC

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
SSLv2 and SSLv3 with RC2 or RC4 encryption	SSLv2 with DES or 3DES SSLv3 with DES or 3DES	SSLv3 with DES or 3DES	SSLv3 with DES or 3DES	SSLv3 with DES or 3DES	
Activities, Platforms, Operational Environments		All			

Table 3-10. WWW Encryption Implementations

3.4.4.5 VPN Encryption

VPN encryption can be provided at zone 1 as well as zones 2, 3, and 4. By placing VPN encryption in zone 1, data can be secured end-to-end. This can provide an extremely high level of security, especially in situations where LAN cables are not fully secured. See Section 3.4.1.2 for guidance on VPN encryption.

3.4.4.6 Content Security Checking

Content security checking can also be provided at zone 1. In many situations, full content checking in zones 2, 3, and 4 may not be possible due to VPN or application layer encryption. In addition, only zone 1 based content security checking can be used to protect workstations from malicious programs that are imported on floppy disks, CDROM, ZIP drives, tapes, or other removable media. The DoD-wide virus detection tool license allows installation of the DoD licensed tools on home computers as well. Checking content on these computers (which may not be behind appropriate zone 2, 3, and 4 protections) before moving the content to official Navy and Marine Corps computers can help protect Navy and Marine Corps workstations.

Best Practices

All DON PC based workstations and servers (including those using the Windows NT, Windows 95, Windows 98, and Macintosh operating systems) should employ content security checking mechanisms from the DoD-wide virus detection tool site license. Content security checking mechanisms should be configured to run in a background mode and scan files upon access. Updated virus detection signatures should be downloaded and installed monthly from the http://infosec.navy.mil or http://infosec.navy.smil.mil web site.

DON organizations should strongly encourage DON employees to install the DoD-licensed antiviral software on the employees' home computers. Organizations should publicize that this software is available free for home use of DON employees.

DON organizations should consider implementing procedures requiring files to be virus scanned before they are attached to outgoing e-mail. A record of the time and date of the scan as well as the tool used should be included in the body of the e-mail.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	DoD site license virus detection tools	DoD site license virus detection tools	DoD site license virus detection tools	DoD site license virus detection tools	
Activities, Platforms, Operational Environments		All			

Table 3-11. Content Security Checking Implementations

3.5 Public Key Infrastructure

The defense in depth approach to information protection for DON information systems is based on the application of numerous complementary and redundant security mechanisms. In addition, infrastructure components are required to support and manage these security mechanisms. The most critical of these components is a Public Key Infrastructure (PKI) required to support the multiple encryption mechanisms that can be applied in the various zones (e.g. VPN encryption, SMIME, SSL).

A public key infrastructure is a collection of components that support the generation and distribution of digital certificates, issuance of Certificate Revocation Lists (CRLs), and the building and running of directories to serve these certificates and CRLs. In order to understand the operational issues and to develop the proper policies associated with operating a PKI, a number of Naval, DoD, and other government entities are operating PKI pilot projects based on commercial standards. These pilots are called “medium assurance” PKI pilots based upon the level of assurance postulated in the digital signatures associated with the certificates. The Defense Message System (DMS) project is fielding a separate PKI based partially on commercial standards and partially on DMS unique standards (this pilot project is sometimes called a “high assurance” PKI).

A digital certificate is an electronic proof of identity that can be used to sign electronic documents, to authenticate the holder of the certificate, and to allow decryption of information intended to be read by the holder of the certificate. Digital certificates are used in many commercial products (e.g., SSL for WWW security, S/MIME for e-mail security) and are based on the use of public key cryptography. In a public key cryptographic system, a person (e.g., using a web browser) generates a public key/private key pair. The private key is never revealed to anyone and is protected by the application that generated it (in our example, the browser). The public key can then be published (e.g., in an X.500 database).

In order to avoid the problem of hostile impersonators publishing public keys under false names, a person’s name and public key are placed in an electronic document and the document is digitally signed by a widely recognized trusted agent. The agent’s signature binds the person’s name to the person’s public key by virtue of the integrity protection provided by the digital signature. This document is called a *digital certificate* and serves as an electronic credential. Anyone accessing the certificate can (1) verify the signature of the trusted agent and, thereby, verify that the public key and the associated identity have not been modified, (2) know that information encrypted with the public key can only be decrypted by the person (or organization) named in the certificate, and (3) check documents signed by the person to verify the person’s signature. The trusted agent that signs the digital certificate is called a *certificate authority (CA)*. In generating a digital certificate, the CA should carefully verify the associated person’s identity in order to provide the required validity of the certificate. This verification is often performed by another entity called a registration authority (RA). The RA communicates the results of the identity verification to the CA before a certificate is issued.

The certification authority sets necessary restrictions on a digital certificate (e.g., the time interval over which the certificate is valid, typically a year for commercial CAs) and revokes the certificate when appropriate (e.g., when an employee leaves an organization or is no longer authorized to sign documents). The CA publishes a certificate revocation list that can be checked by applications (and persons) when validating a certificate from another entity (i.e., before making purchases from an on-line catalogue company). Persons who rely on digital certificates as proof of identity (signature) and integrity should also check to determine the certificate’s period of validity. And finally, persons who rely on digital certificates must trust that the issuer of the certificate (the CA and possibly the RA) has followed acceptable procedures verifying the identity of the certificate holder. Since a digital signature may be used to sign a legally binding document, strict standards for the certificate issuing process are required.

Certificates and certificate revocation lists are generally stored in a publicly accessible directory that is often based on the X.500 and/or the Lightweight Directory Access Protocol (LDAP).

The X.509 standard specifies the structure and contents of a digital certificate. It includes a number of required fields (including name and public key) and optional fields. Most commercial products that use certificates, require certificates to conform to this standard. However, owing to differences in how certificates are used (differences between SSL and S/MIME for example), the content of the optional fields and their uses may vary. The DMS certificate format is based on a variation of the X.509 standard.

Standards for a CA include definitions of the various identity verifications, certificate issuing, certificate management (including revocation), and due diligence procedures for a CA and any associated registration authorities. These procedures and processes are defined in a standards document called a Certification Practices Statement (CPS).

In order to provide a uniform level of confidence in the signatures for the certificates issued by the various government PKI's, procedures must be standardized. The government PKI pilots are expected to develop a standard CPS for government PKI. Examples of possible certificate issuance and certificate revocation processes are illustrated in Figure 3-6 and Figure 3-7. These may not be representative of the certificate issuance and certificate revocation processes that evolve from the government PKI pilots.

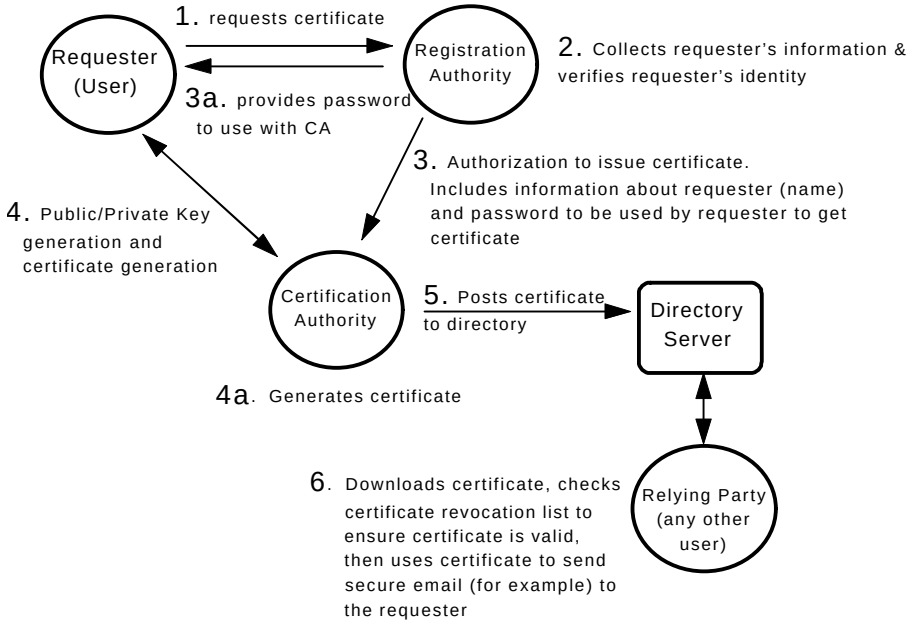

Figure 3-6. Example Certificate Issuance Process

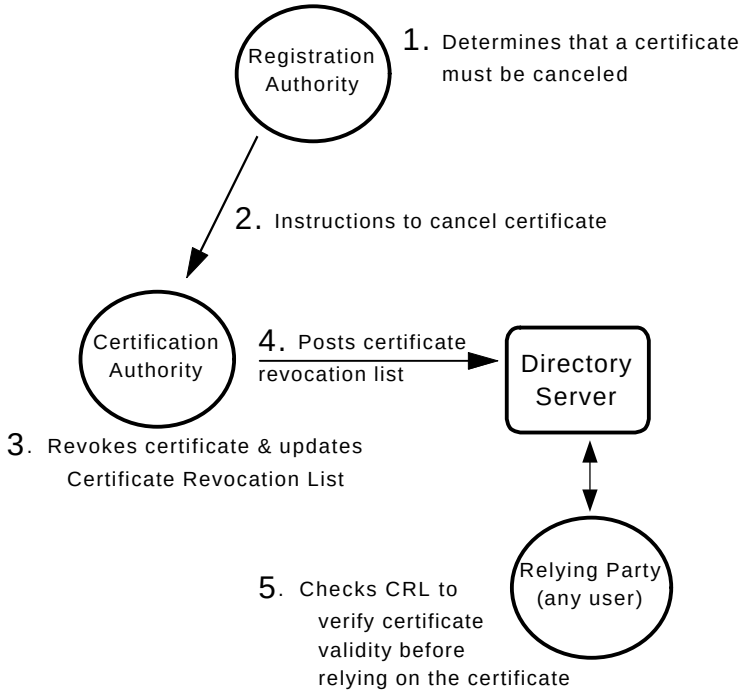

Figure 3-7. Example Certificate Revocation Process

The standards for a PKI also include the standards for the protocols and algorithms used in the communication between and among the CA, RA, and end users' applications. Commercial standards bodies are still developing many of these protocol standards.

Products based on public key cryptography store the private key of the end-user in the product (e.g., a web browser stores the user's private key). An industry standard for securely moving private keys between applications (e.g., between a web browser and a secure e-mail package) is emerging. The use of this standard allows a person to own a single personal digital certificate rather than requiring a different certificate for each application program. The standard is published as part of the Public Key Cryptography Standards (PKCS) of RSA Data Security, Inc. It has been designated PKCS 12.

Best Practices

Owing to the lack of PKI standards, Navy and Marine Corps organizations desiring to use certificate-based public key technologies (e.g. S/MIME, SSL) should coordinate with SPAWAR PMW-161 to either join an ongoing Naval or DoD pilot project or to start a new pilot project.

Navy and Marine Corps organizations using digital certificates should use X.509v3 certificates whenever possible. If possible, the CA's signature should be based on the Digital Signature Standard (DSS). However, until more DSS-based products are available, a signature based on the RSA algorithm is also acceptable.

Naval organizations should use PKCS 12 when private keys are shared between applications.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	X.509v3 certs RSA or DSS for CA signature PKCS12 for key sharing	X.509v3 certs RSA or DSS for CA signature PKCS12 for key sharing	X.509v3 certs RSA or DSS for CA signature PKCS12 for key sharing	X.509v3 certs RSA or DSS for CA signature PKCS12 for key sharing	
Activities, Platforms, Operational Environments	All				

Table 3-12. Public Key Infrastructure Implementations

3.6 Use of Commercially Available Cryptography

Encryption is utilized in numerous information protection mechanisms in all zones and in infrastructure components required to support these mechanisms. This section provides an overview of the best commercial practices in cryptography to protect information (both unclassified information and classified information that will be handled at its original classification level[2]), to make and verify digital signatures, to verify the integrity of information, and to provide other business oriented cryptographic functions. The standards and guidance specified in this section apply to all infrastructure components and information protection mechanisms that make use of cryptography.

The use of cryptography is just one piece of an overall protection strategy. Each piece of the strategy must be considered when determining the level of risk associated with the use of the strategy. Whether or not a particular type of cryptography meets the risk management needs of a particular application depends on many factors, including the strength of the cryptographic algorithm, correctness of the algorithm and associated key management implementation, and the security of the associated *cryptographic protocol*.

The availability and usability of commercial cryptography and security products is increasing. Available products and cryptographic algorithms vary widely in strength and in the quality of implementation. Many commercial cryptographic products are insufficiently strong to provide even weak protections (or signatures, or integrity, etc.). Even many of the products that incorporate strong cryptography allow the cryptography to be used in weak ways. Careful selections of algorithms, of protocol standards, and of product configuration options are all necessary for acceptable security protections.

The following sections provide an overview of cryptography, discuss the acceptable encryption algorithms, and discuss the options required for the secure use of these algorithms. Navy and Marine Corps commands contemplating the use of cryptography for unclassified applications should use the options specified here.

[2] Cryptography used to declassify DoD classified information must be approved by NSA. Contact the Navy INFOSEC Program Office, SPAWAR PMW-161 for further information.

3.6.1 Overview of Cryptography

Cryptographic systems can be divided into two primary types. *Symmetric cryptographic systems* (or secret or private key systems) require the sender and any receivers of a document to have the same key. Securely distributing the secret key to everyone who needs it has historically been a major difficulty with symmetric cryptographic systems. In contrast, *public key cryptographic systems* (also called asymmetric systems) use different keys for the encryption and decryption functions. The encryption key can be made public, allowing anyone with access to the public key to encrypt information intended to be read only by the holder of the private decryption key. If a public key system is used in reverse, it can be used to verify the identity of an information source. The holder of the private key uses it to encrypt information; anyone with access to the public key can decrypt, but since only one person holds the private key, the encrypted document can be tied to the holder of the private key.

In practice, public and private key technologies are often used together. The public key system is used to transmit keys that are then used in a symmetric cryptographic scheme. Public key systems are also used to sign documents. In a typical application, the information to be signed is compressed using a *message digest algorithm* (also called a *secure hash algorithm*). The compressed message (the *message digest*) is signed by being encrypted with the private key piece of a public key scheme. Anyone receiving the document can recompute the message digest, then check the signature using the sender's public key. If the locally computed digest matches the one that arrived with the message, a receiver can determine the identity of the sender (i.e., the document's authenticity) and that the message was not modified en route (i.e., the document's integrity).

A digital signature is a cryptographically produced sequence that a recipient can use in good faith (and hopefully with as low risk as a paper signature) as evidence that a particular person signed an electronic document. Digital signatures are made by using both public key cryptography and message digest algorithms. The document to be signed is put through a message digest function, then the message digest is encrypted with the signer's private key, and the encrypted digest is appended to the document. A recipient uses the signer's public key to decrypt the message digest, puts the document through the same message digest algorithm used by the sender, and if the decrypted digest matches the newly computed digest, concludes that the document arrived unmodified, and that the sender had signed the document.

3.6.2 Standards for Symmetric Encryption Algorithms

The official U.S. government standard for the protection of unclassified information by cryptography is the Data Encryption Standard (DES). DES is the most widely used cryptographic algorithm in the world. Many other symmetric algorithms have been developed commercially, often to meet a perceived need for algorithms that are stronger than DES. However, only a very few of these algorithms have been intensively cryptanalyzed and few have existed long enough to have confidence in their security.

Data Encryption Standard (DES)

As the official U.S. Government standard algorithm for the protection of unclassified information, DES is widely available in commercial products.

Best Practices

DES is currently the preferred symmetric encryption algorithm for the protection of Naval unclassified information. Navy and Marine Corps users should select DES-based products that have been evaluated for proper implementation and operation in accordance with NIST FIPS PUB 140-1, *Security Requirements For Cryptographic Modules*.

DES can be used in a variety of modes. Generally, if a product includes an option for the DES mode, Navy and Marine Corps users should not use DES in the Code Book mode. Other modes have superior security properties.

If a product includes DES and other symmetric algorithms, DES should be used in lieu of the other algorithms unless a careful, risk management analysis is made that determines one of the other algorithms provides lower risk. If an algorithm other than DES is contemplated, it should be selected from the other symmetric algorithms defined in the ITSG and the algorithm should be configured according to the guidance given herein (e.g., key length, number of rounds).

Triple DES

A non-government-standardized variant on the DES algorithm is triple-DES (or 3DES). This scheme encrypts by applying the DES algorithm three times, with three different keys in an attempt to make the key size larger (DES key size is 56 bits, triple-DES is 168 bits) and the cryptography harder to break. The security of the scheme may be better than normal 56 bit DES and is almost certainly no worse. No NIST FIPS for the use of triple-DES exists.

Best Practices

Navy and Marine Corps users may select triple-DES in lieu of DES in applications.

Skipjack (Fortezza)

The Skipjack algorithm is an algorithm developed by NSA and built into Fortezza cards. A number of commercial products can use Skipjack (via the Fortezza card) for symmetric encryption. Many of these products are associated with the Defense Message System program. The Skipjack algorithm is currently classified and so is only available in hardware form. However, the NSA has recently signaled its intent to provide software versions of Skipjack to builders of commercial information processing products. It is unknown at this time whether the FIPS 140-1 quality standard would be applied to these software implementations, or whether NSA and/or NIST will develop a new evaluation standard.

Best Practices

Navy and Marine Corps users may use Skipjack/Fortezza in lieu of DES. However, when commercial products appear that incorporate software versions of Skipjack, the potential user of the product should ensure the product meets whatever quality standard that NIST or NSA has defined (in order to ensure the implementation is correct).

Other symmetric algorithms

Many other symmetric algorithms may be found in commercial products. The security of some of these algorithms is poor and the security of other algorithms may be unknown (not sufficiently cryptanalyzed).

Best Practices

No other symmetric encryption algorithms are approved for Naval use.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
Proprietary or other unlisted algorithms	DES 3DES Skipjack	DES 3DES Skipjack	DES 3DES Skipjack	DES 3DES Skipjack	
Activities, Platforms, Operational Environments		All			

Table 3-13. Symmetric Encryption Algorithm Implementations

3.6.3 Standards for Public Key Cryptography

The current standards for public key cryptography are not issued by a recognized standards body, but are issued by RSA, Incorporated. The IEEE is developing an IEEE standard for public key cryptography (IEEE P1363: Standard for Public-Key Cryptography) that was issued as a first draft on December 19, 1997 and is expected to be finalized soon. Until the IEEE standard is issued, the RSA standards will be used.

RSA Public Key Cryptographic Algorithm

Many commercial products use RSA cryptography as part of a digital signature scheme and as a way of encrypting and distributing keys that are used in symmetric algorithms (e.g. DES). In the cryptographic literature, the RSA algorithm is considered quite strong as long as appropriate key lengths are selected. No federal government standard exists for the use of RSA. The digital signature standard, FIPS pub 186, defines a digital signature scheme that is NOT based on RSA.

Best Practices

Since the DSS is not yet incorporated into many commercial products, the RSA digital signature is acceptable for use when DSS is not available, but only for a limited time (see Section 3.6.5 on digital signatures).

The use of RSA is acceptable for key exchange and key protection applications.

The minimum key length for Naval applications using RSA is 1024 bits. Longer key lengths provide more protection so longer key lengths should be considered when making risk management decisions about an overall system design.

The use of RSA to protect key material should be done in accordance with both the RSA, Inc. specification for the RSA algorithm and the RSA, Inc. specification for cryptographic message syntax (PKCS #1 and PKCS #7).

Diffie Hellman (DH) key agreement standard

The Diffie Hellman key agreement algorithm is another way of securely exchanging a key that then is used in a symmetric algorithm. It is not widely fielded in commercial products (although the Digital Signature Standard (DSS) is based on a variation of DH).

Best Practices

Navy and Marine Corps users may use the Diffie Hellman key agreement algorithm.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
RSA with less than 1024 bit length Other unlisted algorithms	RSA (1024 bit or longer) for key exchange and protection DH RSA (1024 bit or longer) for digital signature	RSA (1024 bit or longer) for key exchange and protection DH	RSA (1024 bit or longer) for key exchange and protection DH	RSA (1024 bit or longer) for key exchange and protection DH	
Activities, Platforms, Operational Environments		All			

Table 3-14. Public Key Cryptography Implementations

3.6.4 Standards for Message Digest Algorithms

A variety of message digest algorithms exists. The two most widely used are the Secure Hash Algorithm - 1 (SHA-1), which is the NIST Standard for message hashing that is used in the NIST Digital Signature Standard (DSS), and the Message Digest-5 (MD5) which was developed by RSA laboratories and is used in many commercial products.

NIST Secure Hash Standard (SHA-1)

SHA-1 (also called just SHA) is the NSA designed, NIST issued federal standard for message digest functions. It is thought to be the strongest widely available message digest algorithm in common use. NIST Federal Information Processing Standard Publication 180-1 says about the

use of SHA-1, “This standard is applicable to all Federal departments and agencies for the protection of unclassified information that is not subject to Section 2315 of Title 10, United States Code, or Section 3502(2) of Title 44, United States Code. This standard is required for use with the Digital Signature Algorithm (DSA) as specified in the Digital Signature Standard (DSS) and whenever a secure hash algorithm is required for Federal applications.”

Best Practices

When a choice of message digest algorithms is available (for example in the emerging S/MIME v3 e-mail security standard), SHA-1 should be selected in lieu of other available message digest algorithms.

Message Digest-5 (MD5)

MD5 was developed by RSA laboratories and is in widespread use in commercial products. Open literature cryptanalysis suggests MD5 may have weaknesses.

Best Practices

If no other choice is available in a commercial product, MD5 may be used. If a choice is available, the SHA-1 should be used.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
Other unlisted algorithms	SHA-1 MD5	SHA-1	SHA-1	SHA-1	
Activities, Platforms, Operational Environments		All			

Table 3-15. Message Digest Algorithm Implementations

3.6.5 Digital Signatures

The two most widely used signature algorithms are the NIST Digital Signature Standard (DSS) and the RSA digital signature. DSS uses the SHA-1 digest algorithm (a government standard) and the El Gamal modified Diffie Hellman as the public key algorithm. RSA digital signature uses MD5 to calculate the message digest and RSA as the public key algorithm.

NIST Digital Signature Standard (DSS)

DSS is the NSA designed, NIST standard for digital signatures. The signature standard uses the SHA-1 hash algorithm and is thought to be stronger than methods based on weaker hash algorithms (for example, signatures based on MD-5). The NIST FIPS PUB 186 that defines the standard states:

"This standard is applicable to all Federal departments and agencies for the protection of unclassified information that is not subject to Section 2315 of Title 10, United States Code, or Section 3502(2) of Title 44, United States Code. This standard shall be used in designing and implementing public-key based signature systems which Federal departments and agencies operate or which are operated for them under contract. Adoption and use of this standard is available to private and commercial organizations."

Best Practices

When selecting a signature standard, Naval organizations should use the DSS whenever possible. This means it should be enabled in commercial products (for example in SSL for web transactions), should be specified when purchasing commercial products for Naval use, and should always be used when Navy and Marine Corps unique products are developed.

RSA Signatures

Digital signatures based on the RSA algorithm typically use the MD5 message digest algorithm with RSA public key algorithm although a growing list of applications use SHA-1 with RSA. This signature scheme is very widely used in commercial products owing to the long lag between the development of RSA digital signatures and the DSS.

Best Practices

Whenever possible, Navy and Marine Corps users should select products that use the DSS. However, in situations where DSS products are not yet available, Navy and Marine Corps users may use RSA signatures. If RSA is used, the SHA-1 message digest algorithm should be selected over the MD-5 message digest algorithm wherever possible. When more products provide implementations of the DSS, the use of RSA signatures will be disallowed.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
Other unlisted algorithms	DSS RSA with SHA-1	DSS	DSS	DSS	
Activities, Platforms, Operational Environments		All			

Table 3-16. Digital Signature Implementations

3.7 References

DES

National Institute of Standards and Technology (NIST), "Data Encryption Standard" Federal Information Processing Standards Publication 46-2 (FIPS PUB 46-2), 30 December 1993

National Institute of Standards and Technology (NIST), “DES Modes of Operation” Federal Information Processing Standards Publication 81 (FIPS PUB 81), 2 December 1980

National Institute of Standards and Technology (NIST), “Security Requirements For Cryptographic Modules” Federal Information Processing Standards Publication 140-1 (FIPS PUB 140-1), 11 January 1994

DH

RSA Data Security, Inc., Public Key Cryptography Standard 3 (PKCS #3), Diffie-Hellman Key-Agreement Standard, Version 1.4, 1 November 1993, http://www.rsa.com/rsalabs/pubs/PKCS/ (23 May 1998)

DoD Wide Virus Detection Tool Site License

Space and Naval Warfare Systems Center (SPAWAR) PMW 161 Information Security (INFOSEC) web page: http://infosec.spawar.navy.mil (Internet) (23 May 1998) or http://infosec.navy.smil.mil (SIPRNET)

DSS

National Institute of Standards and Technology (NIST) “Digital Signature Standard (DSS)” Federal Information Processing Standards Publication (FIPS PUB) 186, 19 May 1994

Firewall Compatibility Requirements

Space and Naval Warfare Systems Command (SPAWAR) PMW-161 report,; “Firewall Services”, December 1996. ftp://infosec.navy.mil/pub/docs/navy/NSS/firewalls/fw_serv.doc

Cheswick, Bellovin; Firewalls and Internet Security; Addison-Wesley Publishing Company Reading MA; 1994

IPSEC

Metzger (Piermont) , Simpson (Daydreamer); “IP Authentication using Keyed MD5” (RFC 1828), August 1995. http://ds.internic.net/rfc/rfc1828.txt (23 May 1998)

Atkinson (Naval Research Lab); “IP Authentication Header” (RFC 1826) August 1995, ftp://ds.internic.net/rfc/rfc1826.txt (23 May 1998)

Atkinson (Naval Research Lab); “Security Architecture for the Internet Protocol” (RFC 1825). ftp://ds.internic.net/rfc/rfc1825.txt (23 May 1998)

Atkinson (Naval Research Lab) “IP Encapsulating Security Payload (ESP)” (RFC 1827). August 1995; ftp://ds.internic.net/rfc/rfc1827.txt (23 May 1998)

Karn (Qualcomm), Metzger (Piermont), Simpson (Daydreamer); “The ESP DES-CBC Transform” (RFC 1829) August 1995, ftp://ds.internic.net/rfc/rfc1829.txt (23 May 1998)

Krawczyk, Canetti (IBM), Bellare (UCSD); “HMAC: Keyed-Hashing for Message Authentication” (RFC 2104) February 1997, ftp://ds.internic.net/rfc/rfc2104.txt (23 May 1998)

Oehler (NSA), Glenn (NIST); “HMAC-MD5 IP Authentication with Replay Prevention” (RFC 2085). February 1997, ftp://ds.internic.net/rfc/rfc2085.txt (23 May 1998)

Maughan, Schertler, Schneider, Turner; “Internet Security Association and Key Management Protocol.” 10 March 1998, ftp://ftp.ietf.org/internet-drafts/draft-ietf-ipsec-isakmp-09.txt (23 May 1998)

Orman (Univ. of Arizona); “The OAKLEY Key Determination Protocol.” 27 April 1998, ftp://ftp.ietf.org/internet-drafts/draft-ietf-ipsec-oakley-02.txt (23 May 1998)

The resolution of ISAKMP with Oakley. (ftp://ftp.ietf.org/internet-drafts/draft-ietf-ipsec-isakmp-oakley-05.txt)

MD5

Rivest (MIT and RSA Data Security Inc.); “The MD5 Message-Digest Algorithm” (RFC1321) April 1992. http://ds.internic.net/rfc/rfc1321.txt (23 May 1998)

Metzger (Piermont) , Simpson (Daydreamer); “IP Authentication using Keyed MD5” (RFC 1828), August 1995. http://ds.internic.net/rfc/rfc1828.txt (23 May 1998)

Operating System Security

Department of Defense; “Department of Defense Trusted Computer System Evaluation Criteria” (The Orange Book), DoD 5200.28-STD, December 1985.

Space and Naval Warfare Systems Command; “Secure Windows NT Installation and Configuration Guide”, SPAWAR PMW-161 Report, November 1997. ftp://infosec.navy.mil/pub/docs/navy/NT-SECURITY/navynt.zip (23 May 1998)

Space and Naval Warfare Systems Center (SPAWAR) PMW 161 Information Security (INFOSEC) web page: Various document on best commercial practices in UNIX security. ftp://infosec.navy.mil/pub/docs/unix/ (23 May 1998)

RSA Public Key Cryptography

RSA Data Security Inc., “Public Key Cryptography Standard 1 (PKCS #1),” 1998, http://www.rsa.com/rsalabs/pubs/PKCS/ (23 May 1998)

RSA Data Security, Inc., “Public Key Cryptography Standard 7 (PKCS #7), Cryptographic Message Syntax Standard”, 1998, http://www.rsa.com/rsalabs/pubs/PKCS/ (23 May 1998)

SHA-1

National Institute of Standards and Technology (NIST), “Secure Hash Standard” FIPS PUB 180-1, 17 April 1995, http://csrc.nist.gov/fips/ (23 May 1998)

S/KEY

Haller (Bellcore), “The S/KEY One-Time Password System” (RFC 1760), February 1995. http://www.cis.ohio-state.edu/rfc/rfc1760.txt (23 May 1998)

S/MIME

Blake, Ramsdell (Worldtalk); “S/MIME Version 2 Message Specification”(Internet Draft), 4 May 1998, http://www.imc.org/draft-ietf-smime-msg (23 May 1998)

Blake, Ramsdell (Worldtalk) “S/MIME Version 2 Certificate Handling” (Internet Draft), 4 May 1998, http://www.imc.org/draft-ietf-smime-cert (23 May 1998)

SSL

Frier, Karlton (Netscape), Kocher (independent); “The SSL Protocol, Version 3.0” (Internet Draft); 18 November 1996; http://home.netscape.com/eng/ssl3/draft302.txt (23 May 1998)

Triple DES (3DES)